

20.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日 2004年 1月16日
Date of Application:

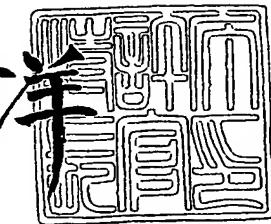
出願番号 特願2004-009861
Application Number:
[ST. 10/C]: [JP2004-009861]

出願人 松下電器産業株式会社
Applicant(s):

2005年 1月28日

特許庁長官
Commissioner,
Japan Patent Office

小川洋



【書類名】 特許願
【整理番号】 2048150057
【あて先】 特許庁長官殿
【国際特許分類】 G06F
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 大森 基司
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 大原 俊次
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 片山 崇
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100109210
 【弁理士】
 【氏名又は名称】 新居 広守
【手数料の表示】
 【予納台帳番号】 049515
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 0213583

【書類名】特許請求の範囲**【請求項 1】**

ネットワークを介してアクセスしてきた、暗号化されたデジタルコンテンツを復号し得る端末装置の中から不正な端末装置を検出する認証用サーバ装置であって、

前記端末装置から、当該端末装置に予め与えられている端末鍵に基づいて生成された検証用のデータと、端末装置毎にその製造後に付加された識別情報である端末IDとを受信する端末情報受信手段と、

前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証手段と、

複数の端末装置について、前記端末IDを含む所定の端末情報を予め保持し、前記受信した端末IDについて検索を試みる端末情報検索手段と、

前記端末鍵検証手段によって前記端末鍵の正当性は確認されたが、前記受信した端末IDと異なる端末IDが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定手段と

を備えることを特徴とする認証用サーバ装置。

【請求項 2】

前記認証用サーバ装置は、さらに、

当該認証用サーバ装置の操作者から端末IDを受け付ける受付手段と、

前記受け付けた端末IDが、前記端末情報検索手段に保持されている端末情報に登録されているか否かを判別する未登録判別手段とを備え、

前記端末情報検索手段は、さらに、

前記未登録判別手段において登録されていないと判別された場合のみ、新たに前記所定の端末情報を追加登録する

ことを特徴とする請求項1記載の認証用サーバ装置。

【請求項 3】

前記デジタルコンテンツについてのアクセス回数は1回に制限されている場合であって、

前記認証用サーバ装置は、さらに、

前記端末鍵および前記端末IDの組によって特定される端末装置毎に、前記アクセスを受け付けたデジタルコンテンツの履歴を表す情報を蓄積する履歴蓄積手段を備え、

前記不正端末判定手段は、さらに、

同一の前記端末鍵および前記端末IDに係る端末装置から、デジタルコンテンツに対して複数回数アクセスを受け付けた場合は、当該端末装置は不正端末であると判定することを特徴とする請求項1又は2記載の認証用サーバ装置。

【請求項 4】

前記端末鍵は、秘密鍵暗号方式における秘密鍵又は公開鍵暗号方式における公開鍵証明書である

ことを特徴とする請求項3記載の認証用サーバ装置。

【請求項 5】

ネットワークを介してアクセスしてきた端末装置の中から不正な端末装置を検出する認証用サーバ装置と、ネットワークを介して前記認証用サーバ装置にアクセスし得る端末装置を含む不正端末検出システムであって、

前記端末装置は、

当該端末装置に予め与えられている端末鍵によって生成された検証用データと、端末装置毎にその製造後に付加された識別情報である端末IDとを前記認証サーバ装置に送信する端末情報送信手段を備え、

前記認証用サーバ装置は、

前記端末装置から、前記端末鍵に基づいて生成された検証用のデータと前記端末IDとを受信する端末情報受信手段と、

前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証手段

と、

複数の端末装置について、前記端末IDを含む所定の端末情報を予め保持し、前記受信した端末IDについて検索を試みる端末情報検索手段と、

前記端末鍵検証手段によって前記端末鍵の正当性は確認されたが、前記受信した端末IDと異なる端末IDが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定手段と

を備えることを特徴とする不正端末検出システム。

【請求項6】

ネットワークを介してアクセスしてきた、暗号化されたデジタルコンテンツを復号し得る端末装置の中から不正な端末装置を検出する不正端末検出方法であって、

前記端末装置から、当該端末装置に予め与えられている端末鍵に基づいて生成された検証用のデータと、端末装置毎にその製造後に付加された識別情報である端末IDとを受信する端末情報受信ステップと、

前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証ステップと、

複数の端末装置について、前記端末IDを含む所定の端末情報を予め保持し、前記受信した端末IDについて検索を試みる端末情報検索ステップと、

前記端末鍵検証ステップによって前記端末鍵の正当性は確認されたが、前記受信した端末IDと異なる端末IDが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定ステップと

を含むことを特徴とする不正端末検出方法。

【請求項7】

前記不正端末検出方法は、さらに、

操作者から端末IDを受け付ける受付ステップと、

前記受け付けた端末IDが、前記端末情報検索ステップに保持されている端末情報に登録されているか否かを判別する未登録判別ステップとを含み、

前記端末情報検索ステップは、さらに、

前記未登録判別ステップにおいて登録されていないと判別された場合のみ、新たに前記所定の端末情報を追加登録する

ことを特徴とする請求項6記載の不正端末検出方法。

【請求項8】

ネットワークを介してアクセスしてきた、暗号化されたデジタルコンテンツを復号し得る端末装置の中から不正な端末装置を検出する認証用サーバ装置のためのプログラムであって、

前記端末装置から、当該端末装置に予め与えられている端末鍵に基づいて生成された検証用のデータと、端末装置毎にその製造後に付加された識別情報である端末IDとを受信する端末情報受信ステップと、

前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証ステップと、

複数の端末装置について、前記端末IDを含む所定の端末情報を予め保持し、前記受信した端末IDについて検索を試みる端末情報検索ステップと、

前記端末鍵検証ステップによって前記端末鍵の正当性は確認されたが、前記受信した端末IDと異なる端末IDが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定ステップと

をコンピュータに実行させることを特徴とするプログラム。

【請求項9】

前記プログラムは、さらに、

操作者から端末IDを受け付ける受付ステップと、

前記受け付けた端末IDが、前記端末情報検索ステップに保持されている端末情報に登録されているか否かを判別する未登録判別ステップとを含み、

前記端末情報検索ステップは、さらに、
前記未登録判別ステップにおいて登録されていないと判別された場合のみ、新たに前記
所定の端末情報を追加登録する
ことを特徴とする請求項 8 記載のプログラム。

【書類名】明細書**【発明の名称】認証用サーバ装置、不正端末検出方法および不正端末検出システム****【技術分野】****【0001】**

本発明は、不正に製造された端末を検出する装置、方法およびそのシステムに関し、特に、不正に復号鍵が生成されたネットワーク上のDVDプレーヤなどを検出する装置等に関する。

【背景技術】**【0002】**

近年、パッケージコンテンツ（例えば、映像、音声ソフトなど）を格納した種々の記録媒体（例えば、DVD（Digital Versatile Disc）など）およびこれらを再生する装置（例えば、DVDプレーヤなど）が普及すると共に、これらの著作権を保護するため、各種の方策が講じられている。

例えば、DVDプレーヤに格納されている端末鍵（「デバイス鍵」ともいう。）を用いて、DVDに記録されている暗号化されたコンテンツを復号する方法がある（従来例1）。この場合、端末鍵は、プレーヤ毎に異なっているものとする。また、ライセンス料の支払いと引き換えに、ライセンサからDVDプレーヤの製造会社に上記ライセンス料に応じた個数の端末鍵が提供される。

【0003】

一方、通信網に接続されているセンタと複数の端末から構成されるグループ鍵を利用する通信システムにおいて、不正に複製された端末を自動的に発見して排除する方法も提案されている（例えば、特許文献1参照）。これは、通信網に接続されているセンタが、端末に新規のグループ鍵を配布する際に、端末から端末IDと端末乱数をセンタの公開鍵で暗号化した情報を受信し、通信ログを検索して、同一端末IDで端末乱数の異なる端末の有無を検査する。該当する端末があれば、複製端末であると判断して、グループ鍵を配布しない。この場合、各端末で発生させる乱数は複製が困難であり、複製された端末は同じ乱数を生成できないので、複製端末の存在を検出することができる。

【特許文献1】特開2002-217890号公報

【発明の開示】**【発明が解決しようとする課題】****【0004】**

しかしながら、上記従来例1の方法では、ライセンス料で規定された個数を越えた数の端末鍵を生成したり、不正な解析によって正当なDVDプレーヤから端末鍵を解読し、解読した端末鍵を埋め込んだDVDプレーヤを不正に複製する場合も生じ得る。その場合、「複数の端末に同一の端末鍵が格納されていること」や「不正なDVDプレーヤに格納されている端末鍵がどの正当なDVDプレーヤの端末鍵なのか」を検出することは困難であるという問題がある。

【0005】

図10は、上記従来例1における問題の概要を説明するための図である。図10に示されるように、機器製造メーカ100は、ライセンサ150に1万台分のライセンス料を支払って正当に1万個の端末鍵（KA1～KA10000）をライセンサ150（又はライセンサ150から委託された鍵管理会社）から受け取って各端末に格納している。

しかし、機器製造メーカ200のように、ライセンサ150に1台分のライセンス料を支払っただけで、1個の端末鍵（KB1）を不正に9999個コピーして1万台の端末に格納することも可能である。さらに、機器製造メーカ300のように、ライセンサ150にライセンス料を支払うことなく、機器製造メーカ200が製造した端末201入手し、その端末に格納されている端末鍵KB1を不正に複製して同一の端末鍵KB1を全端末に格納することも可能である。

【0006】

また、上記特許文献1の方法は、不正に複製された端末か否かを検出することは可能で

あるが、「不正なDVDプレーヤに格納されている端末鍵がどの正当なDVDプレーヤの端末鍵なのか」を検出することは困難である。

そこで、本発明は、複数の端末に同一の端末鍵が格納されていることや不正端末にどの正当な端末の端末鍵が格納されているかを検出し得る認証用サーバ装置、不正端末検出方法などを提供することを目的とする。

【課題を解決するための手段】

【0007】

上記の目的を達成するために、本発明に係る認証用サーバ装置は、ネットワークを介してアクセスしてきた、暗号化されたデジタルコンテンツを復号し得る端末装置の中から不正な端末装置を検出する認証用サーバ装置であって、前記端末装置から、当該端末装置に予め与えられている端末鍵に基づいて生成された検証用のデータと、端末装置毎にその製造後に付加された識別情報である端末IDとを受信する端末情報受信手段と、前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証手段と、複数の端末装置について、前記端末IDを含む所定の端末情報を予め保持し、前記受信した端末IDについて検索を試みる端末情報検索手段と、前記端末鍵検証手段によって前記端末鍵の正当性は確認されたが、前記受信した端末IDと異なる端末IDが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定手段とを備える。

【0008】

これにより、たとえ端末鍵が不正に生成されたり複製されたりした場合であっても、端末鍵に対応づけて登録されている各端末に付加された端末IDが異なる場合は、不正な端末か否かを容易に判定することができる。

さらに、上記目的を達成するために、本発明に係る不正端末検出システムは、ネットワークを介してアクセスしてきた端末装置の中から不正な端末装置を検出する認証用サーバ装置と、ネットワークを介して前記認証用サーバ装置にアクセスし得る端末装置を含む不正端末検出システムであって、前記端末装置は、当該端末装置に予め与えられている端末鍵によって生成された検証用データと、端末装置毎にその製造後に付加された識別情報である端末IDとを前記認証サーバ装置に送信する端末情報送信手段を備え、前記認証用サーバ装置は、前記端末装置から、前記端末鍵に基づいて生成された検証用のデータと前記端末IDとを受信する端末情報受信手段と、前記生成された検証用のデータを用いて前記端末鍵の正当性を検証する端末鍵検証手段と、複数の端末装置について、前記端末IDを含む所定の端末情報を予め保持し、前記受信した端末IDについて検索を試みる端末情報検索手段と、前記端末鍵検証手段によって前記端末鍵の正当性は確認されたが、前記受信した端末IDと異なる端末IDが検索された場合に、前記端末装置は不正な端末であると判定する不正端末判定手段とを備える。

【0009】

これにより、たとえ端末鍵が不正に生成されたり複製されたりした場合であっても、端末鍵に対応づけて登録されている各端末に付加された端末IDが異なる場合は、認証用サーバ装置にアクセスしてきた端末装置が不正な端末か否かを容易に判定することができるので、ネットワークを介して配信されるデジタルコンテンツに対する著作権侵害を最小限に抑えることが可能となる。

【0010】

なお、本発明は、上記認証用サーバ装置が備える特徴的な手段をステップとする不正端末検出方法として実現したり、それらステップをパソコンコンピュータ等に実行させるプログラムとして実現したりすることもできる。そして、そのプログラムをDVD等の記録媒体やインターネット等の伝送媒体を介して広く流通させることができるのは云うまでもない。

【発明の効果】

【0011】

以上の説明から明らかなように、本発明によれば、不正な端末を容易に検出し、ネットワークを介して配信されるデジタルコンテンツに対する著作権侵害を最小限に抑えること

が可能となる。

以上のように、本発明により、端末鍵と端末IDとを組み合わせて検証に用いることによって不正に製造された端末装置の検出をより容易に行うことが可能となり、パッケージコンテンツの著作権を適正に保護することができる。従って、インターネット等のネットワークを介してDVD等に格納されているデジタル著作物の配信や流通が活発になってきた今日において、本願発明の実用的価値は極めて高い。

【発明を実施するための最良の形態】

【0012】

以下、本発明に係る実施の形態について、図面を参照しながら詳細に説明する。

図1は、本実施の形態に係る不正端末検出システム5の概要を示すプロック図である。図1の不正端末検出システム5は、ネットワーク30を利用して不正に製造された端末（例えば、DVDプレーヤなど）を検出するためのシステムであり、上記端末の検出を行うセンタ50の認証サーバ40と検査対象のDVD端末20（少なくとも1台存在している。）とが、例えば、インターネットなどのネットワーク30を介して接続されている。ここで、「不正に製造」とは、正当な権限を有さずに製造することをいい、例えば、暗号化されているコンテンツ（例えば、DVD-ROMに格納されている暗号化されたパッケージソフト）を復号するために必要な端末鍵を、不正な方法で上記パッケージコンテンツを再生するための端末（例えば、DVDプレーヤ）に格納する場合が該当する。

【0013】

ここで、本システム5における不正端末の検出方法の概要について説明する。本実施の形態では、DVD-ROMパッケージ10のユーザの利用形態として、以下の3つの場合を想定する。

(1) DVD-ROMパッケージ10に格納されているコンテンツ（例えば、映画のコンテンツ）そのものを利用する。

(2) 上記(1)のコンテンツに関連するサブコンテンツ（例えば、映画のコンテンツに対する無料の字幕用のデータコンテンツ）をネットワーク30上のセンタ50から入手して利用する。

(3) 上記(1)のコンテンツに関連する暗号化されたサブコンテンツ（例えば、ディレクターズカット映像やおまけ映像など）を、さらに料金を支払ってネットワーク30上のセンタ50から入手して利用する。この場合は、料金を支払うことによって、上記サブコンテンツを復号するための鍵（復号鍵）をセンタ50から入手することとする。

【0014】

そこで、上記(2)および(3)の場合は、ユーザは、DVD端末20を介して必ずセンタ50に接続するため、その際に認証サーバ40を用いて自動的に当該DVD端末20を認証することとする。具体的には、DVD端末20から認証サーバ40にサブコンテンツの送信を要求する際に、いわゆる「チャレンジレスポンス型認証方式」を用いてDVD端末20を認証する。

【0015】

例えば、秘密鍵暗号方式を用いて「チャレンジレスポンス型認証」を行う場合は、認証側（本実施の形態では認証サーバ40）と被認証側（本実施の形態ではDVD端末20）が同一の端末鍵（秘密鍵）を保持する。そして、DVD端末20は、認証サーバ40に認証要求を送信する。DVD端末20から認証要求を受信した認証サーバ40は、乱数を生成してDVD端末20に送信する。DVD端末20は、自身が保持する端末鍵で受信した乱数の暗号化を行い、端末IDと共に認証サーバ40に送信する。DVD端末20から、乱数を暗号化したデータと端末IDとを受信した認証サーバ40は、予め保持している、DVD端末20が保持するものと同一の端末鍵で乱数を復号して、DVD装置20が保持する端末鍵が正当な端末鍵か否かを検証する。さらに、認証サーバ40は、DVD端末20から受信した端末IDが、予め登録している端末IDと一致するか否かを調べる。もし、認証サーバ40からDVD端末20に送信した乱数と認証サーバ40が復号した乱数とが一致しない場合（又は乱数を復号できない場合）、認証サーバ40は、そのDVD端

末20は「不正な端末である」と判定する。特に、乱数は正しく復号できたが、端末IDが一致しない場合は、DVD装置20の端末鍵は「不正に複製された」と判断する。

【0016】

一方、公開鍵暗号方式を用いて「チャレンジレスポンス型認証」を行う場合の一例を以下に示す。認証サーバ40は、証明書発行局の公開鍵を保持している。DVD端末20は、認証サーバ40に、認証要求と共に自身の公開鍵証明書を送信する。認証サーバ40は、保持している証明書発行局の公開鍵を用いてDVD端末20から受信した公開鍵証明書の正当性を検証する。公開鍵証明書が正当なものであると確認した場合、認証サーバ40は、乱数を生成してDVD端末20に送信する。DVD端末20は、自身が保持する端末鍵（秘密鍵）を用いて受信した乱数にデジタル署名を施し、端末IDと共に認証用データとして認証サーバ40に送信する。これにより、認証サーバ40は、検証済みの公開鍵証明書に対応するDVD端末20の公開鍵で、受信した認証用データの正当性を検証する。受信した認証用データの正当性が確認できない場合、認証サーバ40は、DVD端末20は「不正な端末である」と判定し、認証用データの正当性が確認できた場合は、DVD端末20は「正当な端末である」と判定する。

【0017】

なお、「端末鍵」は、個々のDVD端末20によって異なる鍵であり、上記のように秘密鍵暗号方式における秘密鍵（この場合、認証サーバ40とDVD端末20とは、同一の秘密鍵を保有する。）や、公開鍵暗号方式における秘密鍵（この場合、DVD端末20は、認証サーバ40に自身の公開鍵証明書を送信し、認証サーバ40は、受信した公開鍵証明書に含まれているDVD端末20の公開鍵を保持する。）などがある。ここで、「公開鍵証明書」には、DVD端末の「形式+連番」、「端末ID」、「公開鍵」、および「端末IDと公開鍵とを連結したデータに対するデジタル署名」等が含まれることとする。また、「端末ID」とは、DVD端末を識別し得る情報をいい、例えば、ユーザが上記DVD端末20の購入時又はサービスの加入時に登録する際に特定されるユーザIDやサービスIDが該当する。端末IDのその他の例としては、IPアドレスやMACアドレス、ユーザ本人が記入する名前やユーザが任意につけるニックネームなどがある。なお、端末IDは、上記購入時又はサービスの加入時に、既に登録されている他の端末IDと重複していないことを確認して登録することとしてもよい。

【0018】

図2は、本システム5におけるDVD端末20と認証サーバ40の機能構成を示したブロック図である。図2のDVD端末20は、DVD-ROMパッケージ10に格納されているコンテンツの復号及び再生を行う機能を有すると共に、ネットワーク30を介して認証サーバ40から各種のサブコンテンツ入手する機能を有するDVDプレーヤであり、通信制御部21、全体制御部22、復号再生部23、出入力部24及び端末情報記憶部25を備える。なお、DVD端末20における各構成要素は、バス29を介して相互に接続されている。

【0019】

通信制御部21は、ネットワーク30を介して認証サーバ40と通信を行うための制御を行う。全体制御部22は、例えば、RAMやROM等を備えるマイクロコンピュータであり、DVD端末20の全体を制御する。復号再生部23は、DVD-ROMパッケージ10に格納されている、暗号化されているコンテンツの復号および再生を行う。出入力部24は、スイッチ類や液晶パネル等を備え、ユーザからの操作を受け付けると共に、必要な情報をユーザに提示する。端末情報記憶部25は、例えば、セキュアな（対タンパ性を有する）RAMであり、端末鍵（各種の秘密鍵）、公開鍵、公開鍵証明書等や端末IDを記憶する。ここで、許可されていない第3者は、端末情報記憶部25に記憶されている情報を参照したり、更新したりすることができないこととする。

【0020】

一方、図2の認証サーバ40は、ネットワーク30を介してサブコンテンツの入手を要求してきた端末の認証を行うサーバであり、通信制御部41、全体制御部42、端末認証

部43、入出力部44および認証用DB45を備える。なお、認証サーバ40における各構成要素は、バス49を介して相互に接続されている。

通信制御部41は、上記DVD端末20における通信制御部21と同様、認証サーバ40の通信機能の制御を行う。全体制御部42は、例えば、RAMやROM等を備えるマイクロコンピュータであり、認証サーバ40の全体を制御する。端末認証部43は、認証用DB45に格納されている端末鍵や端末ID、DVD端末から受信した端末ID等に基づいて、当該DVD装置を認証する。

【0021】

入出力部44は、キーボードや液晶パネル等を備え、センタ50の管理者等からの操作を受け付けると共に、必要な情報を管理者等に提示する。認証用DB45は、DVD端末毎に端末鍵（各種の秘密鍵）、公開鍵、公開鍵証明書等および端末IDを関連づけて登録し、又は記憶している。

図3は、上記認証用DB45に記憶されているデータの一例を示す。図3(a)は、認証用DB45に記憶されている、DVD端末の形式+連番、端末ID、端末鍵および各DVD端末が行ったサブコンテンツの送信要求履歴を対応付けて格納するためのテーブル例である。この「形式+連番」により、DVD端末を識別することができる。なお、図3(a)の形式+連番、端末鍵は、DVD端末が製造された時点で確定するデータであり、端末IDは、上述したように、購入時又はサービスの加入時に確定（製造後に認証サーバ40に登録）するものとする。

【0022】

また、図3(b)は、上記認証用DB45に憶されている、DVD端末の形式、端末鍵の総数およびアクセス数を対応付けて格納するためのテーブル例である。

【0023】

次に、以上のように構成される不正端末検出システム5の動作について説明する。図4は、上記の利用形態(2)、即ち、DVD端末20が無料のサブコンテンツ入手する場合のDVD端末20—認証サーバ40間における通信シーケンス図である。

【0024】

最初に、DVD端末20は、認証サーバ40にサブコンテンツの送信要求を行う(S302)。これにより、認証サーバ40は、乱数Rを生成し(S304)、DVD端末20に送信する(S306)。すると、DVD端末20は、端末情報記憶部25に記憶している端末鍵と端末IDを読み出し、端末鍵(SK_X)で、受信した乱数Rを暗号化(=Res)し(S308)、このResと端末ID(ID_X)とを認証サーバ40に送信する(S310)。

【0025】

次に、認証サーバ40は、DVD端末20から受信した暗号化された乱数R及び端末IDについて検証し、DVD端末20が正当な端末か否かを認証する(S312:認証処理1)。DVD端末20が正当な端末であると判定した場合、認証サーバ40は、DVD端末20に対して要求通りのサブコンテンツを送信する(S314)。もし、DVD端末20が不当な端末であると判定した場合、認証サーバ40は、DVD端末20に対して、エラーに応じて特定したエラーメッセージを送信する(S314括弧書き)。

【0026】

一方、DVD端末20は、認証サーバ40からサブコンテンツを受信した場合は、これを記録又は再生し(S316)、エラーメッセージを受信した場合は、入出力部24にエラーメッセージを表示する(S316)。

エラーメッセージとしては、例えば、「この端末では、本サービスを受けることができません。」、「この端末は、いずれROMパッケージの再生もできなくなります。」というメッセージ又は警告等を現地語（例えば、DVD端末が販売される地域の言語など）で表示する。

【0027】

なお、エラーメッセージとしての表示ではないが、コンテンツによっては、定期的に更

新される無料の「おまけコンテンツ」を提供するというサービスもあり、この場合は、定期的に端末がセンタに自動でアクセスを行うため、入出力部24に、「おまけコンテンツの自動更新を行うため、ネットワークを接続した状態にしておいて下さい。」等の表示を行い、上記認証の実施を確保することとしてもよい。

【0028】

また、図5は、上記の利用形態(3)、即ち、DVD端末20が有料のサブコンテンツを入手する場合のDVD端末20-認証サーバ40間における通信シーケンス図である。なお、図5においては、認証処理1(S312)までは、上記図4と同じ処理であるため、説明を省略する。

認証サーバ40は、DVD端末20から要求されたサブコンテンツが有料か否かを判別し、有料の場合は、DVD端末20に対して料金の支払い要求を行う(S322)。「料金の支払い要求」を受信したDVD端末20は、料金支払処理を実行し(S324)、認証サーバ40に料金支払済み通知を行う(S326)。

【0029】

DVD端末20から「料金支払済み通知」を受信した認証サーバ40は、DVD端末20にサブコンテンツ(又はエラーメッセージ)を送信する(S314)。なお、以下の処理は、図4におけるS312の処理と同じであるため、図5においては省略している。

図6は、上記図4及び図5に示した、認証サーバ40における認証処理1(S312)の処理内容を示すフローチャートである。

【0030】

最初に、端末認証部43は、通信制御部41を介してDVD端末20から端末ID(ID_X)と暗号化された乱数R(=R_{es})とを受信すると、認証用DB45に保持している、DVD端末20と同一の端末鍵(ID_X)で暗号化された乱数Rを復号する(S402)。

復号した結果、乱数Rが正しくない(又は復号できない)場合(S404:N_o)、端末認証部43は、DVD端末20が正しい端末鍵を有さないDVD端末であると判定し、その旨のエラーメッセージ等を特定し、警告通知を行なうことを決定する(S410)。

【0031】

一方、復号した結果、乱数Rが正しい場合(S404:Y_es.)、端末認証部43は、さらに、乱数Rの復号に用いた端末鍵とDVD端末20から受信した端末ID(ID_X)との組について認証用DB45を検索する(S406)。そして検索した結果、上記端末鍵に対応する端末ID(ID_X)がある場合(S408:N_o)、端末認証部43は、上記端末IDおよび暗号化された乱数Rを送信してきた端末は「正当な端末」であると判定してネットワークの接続を許可すること(以下、「ネット接続許可」という。)を決定する。

【0032】

しかし、受信した端末IDが上記端末鍵に対応する端末IDでない場合(S408:Y_es.)、端末認証部43は、「複数のDVD端末に同一の端末鍵が格納されている」と判定してエラーメッセージ等を特定し、上記DVD端末20に警告通知を行なうことを決定する(S414)。

以上のように、本実施の形態に係る認証サーバによれば、上記の端末鍵と端末IDとを組み合わせて端末の認証に使用することにより、より確実に不正な端末か否かを判別することが可能となる。

【0033】

(変形例1)

上記実施の形態においては、認証サーバ40が、DVD端末20から受信した暗号化された乱数Rおよび端末IDに基づいて、当該DVD端末20が正当か否かを判定する実施例について説明したが、異なるDVD端末が、同一の端末鍵および同一の端末IDを有している場合は、それらのDVD端末が正当か否かを判別することは困難である。そこで、本変形例では、無料のサブコンテンツを受信できる回数が1回に限定されており、同一の

端末鍵および同一の端末IDを有するDVD端末から複数回アクセスがあった場合は、当該端末は「複製された端末鍵を有する不正な端末」とすると判定する。例えば、端末鍵の総数が10,000であるのに、18,500回のアクセスがあった場合が該当する（上記図3（b）参照）。

【0034】

図7は、本変形例における、上記図4又は図5の認証処理（S312）の処理内容を示すフローチャートである。上記図4又は図5のフローチャートと異なる点は、認証用DB45を参照して過去に同一のサブコンテンツの送信要求があった場合は（S502：Yes）、当該DVD端末は「複製された端末鍵を有する不正な端末」とると判定する点である。

【0035】

以上のように、本変形例における認証サーバによれば、たとえ、同一の端末鍵および同一の端末IDを有するDVD端末が複数ある場合は、アクセス回数を計数することによって不正な端末か否かを判別することが可能となる。

【0036】

（変形例2）

上記の実施の形態においては、予め認証サーバとDVD端末が共有する秘密鍵（共通鍵）を用いて、認証サーバがDVD端末から受信した暗号化された乱数Rおよび端末IDに基づいて、当該DVD端末が正当な装置か否かを判定する実施例について説明したが、本変形例では、公開鍵暗号方式を用いて不正な端末を検出する実施例について説明する。本変形例の場合、端末IDと端末鍵との組は、認証サーバとの認証後に登録することとしてもよいこととする。

【0037】

なお、本変形例における認証サーバ及びDVD端末の機能構成は、公開鍵暗号システム及びデジタル署名を用いる以外は、上記実施の形態における認証サーバ40及びDVD端末20と同じである。

【0038】

図8は、本変形例の認証サーバ40-DVD装置20間における通信シーケンス図である。

最初に、DVD端末20は、認証サーバ40にサブコンテンツの送信要求を行う（S302）。これにより、認証サーバ40は、Cert_Xを送信するようにDVD端末20に要求する（S802）。ここで、「Cert_X」とは、端末ID、端末鍵（SK_X）に対応する公開鍵（PK_X）と上記端末IDと公開鍵とを連結したデータに対する認証局CA（図示せず）のデジタル署名（Sign_X）を含むデータをいう。

これにより、DVD端末20は、生成したCert_Xを認証サーバ40に送信し（S804、S805）する。

【0039】

次に、DVD端末20からCert_Xを受信すると、認証サーバ40は、証明書確認用公開鍵（PK_CA）を用いてCert_X内のデジタル署名Sign_Xが、公開鍵（PK_X）と端末IDとを連結したデータに対するデジタル署名であるか否かを検証する（S810）。ここで、Sign_Xが正当であると確認できた場合、認証サーバ40は、乱数Rを生成してDVD端末20に送信する（S812）。

【0040】

すると、DVD端末20は、装置内に保有する端末鍵（SK_X）で乱数Rに対してデジタル署名を施して（=Sign_R）（S814）、認証サーバ40に送付する（S816）。

この後、認証サーバ40は、上記のように受信した端末ID、公開鍵について認証を行なう（S818）。

【0041】

認証の結果、上記端末ID及び公開鍵の正当性が確認できた場合は、DVD端末20に

サブコンテンツを送信する（S314）。一方上記端末ID及び公開鍵の正当性が確認できない場合は、DVD端末20にエラーメッセージを送信する（S818括弧書き）。なお、DVD端末20側で、サブコンテンツを受信する（又はエラーメッセージを表示する）処理（S316）は、上記、図4又は図5の場合と同様である。

【0042】

図9は、上記図8における認証処理2（S818）の流れを示すフローチャートである。

- 最初に、認証サーバ40は、端末鍵（SK_X）に対応する公開鍵（PK_X）で上記Sign_Rが、乱数Rに対する端末鍵（SK_X）によるデジタル署名であるか否かを検証する（S902）。この場合、Sign_Rが正当であると確認できない場合は（S903：No）、本認証を中止してその旨をDVD端末20に通知する（S904）。

【0043】

一方、Sign_Rが正当であると確認できた場合（S903：Yes）、認証サーバ40は、DVD端末20の端末IDと公開鍵との組の有無について、認証用DB45を検索する（S905）。

ここで、もし、同一の公開鍵がない場合は（S906：No）、新規な正当なDVD端末であると判断し、上記端末ID及び公開鍵を認証用DB45に登録し、ネット接続の許可を決定する（S914）。

【0044】

一方、公開鍵については同一のものがあったが、端末IDについては異なっていた場合は（S908：No）、複数のDVD端末に同一の端末鍵が格納されていると不正な端末であると判断し、その旨の警告を通知することとする（S910）。なお、公開鍵も端末IDも同一のものが存在する場合は、当該DVD端末は正当な端末であると判定し、ネット接続の許可を決定する（S914）。

【0045】

なお、上記実施の形態に係る不正端末検出システム5においては、センタ50が1ヶ所の場合の実施例について説明したが、センタが複数ある場合であっても、上記端末鍵および端末IDの組の情報を全てのセンタで共有することによって（例えば、端末鍵および端末IDの組の情報を格納する共通のサーバを用意する。）、本発明を適用することが可能である。

【0046】

さらに、上記の実施の形態及び変形例においては、検証端末としてDVD端末を例に挙げて説明したが、DVD端末に限定するものではなく、CDプレーヤやパーソナルコンピュータ等、デジタルコンテンツに関して各種暗号システムを適用し得る装置であってよい。

【産業上の利用可能性】

【0047】

本発明の認証用サーバ装置、不正端末検出方法および不正端末検出システムは、デジタルコンテンツの著作権を保護しながらネットワークを介して暗号化されたコンテンツを配信し得るコンテンツサーバ装置として適用が可能であり、著作権を保護しながらネットワークを介して暗号化されたコンテンツを配信するネットワークシステムとして有用である。

【図面の簡単な説明】

【0048】

【図1】本実施の形態に係る不正端末検出システムの概要を示すブロック図である。

【図2】不正端末検出システムにおけるDVD端末と認証サーバの機能構成を示したブロック図である。

【図3】(a)は、認証サーバの認証用DBに記憶されているデータの一例を示す。

(b)は、認証サーバの認証用DBに記憶されているデータの一例を示す。

【図4】DVD端末が無料のサブコンテンツ入手する場合のDVD端末-認証サー

バ間における通信シーケンス図である。

【図5】DVD端末が有料のサブコンテンツを入手する場合のDVD端末-認証サーバ間における通信シーケンス図である。

【図6】図4又は図5に示される、認証サーバにおける認証処理1の流れを示すフローチャートである。

【図7】図4又は図5に示される、認証サーバにおける認証処理1の変形例の流れを示すフローチャートである。

【図8】変形例2におけるDVD端末-認証サーバ間における通信シーケンス図である。

【図9】図8に示される、認証サーバにおける認証処理2の流れを示すフローチャートである。

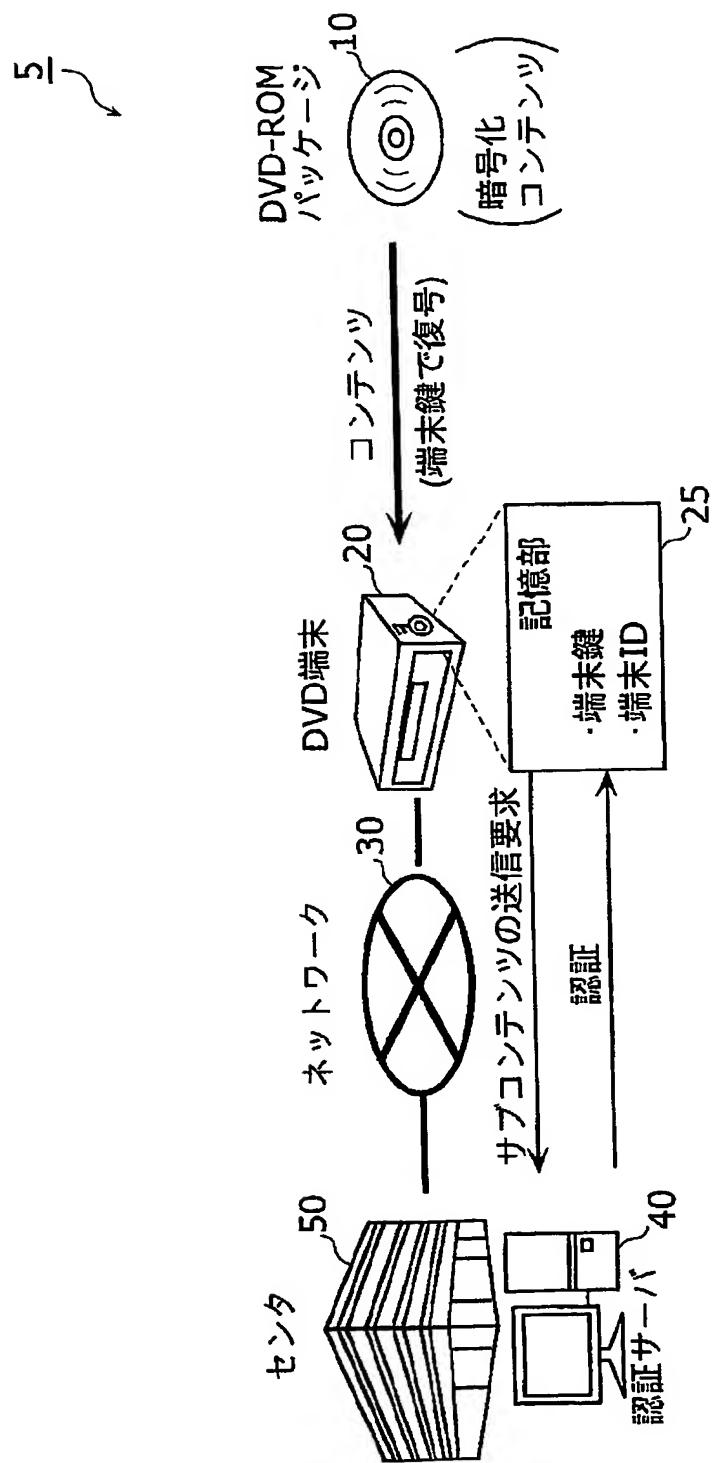
【図10】従来例1における問題の概要を説明するための図である。

【符号の説明】

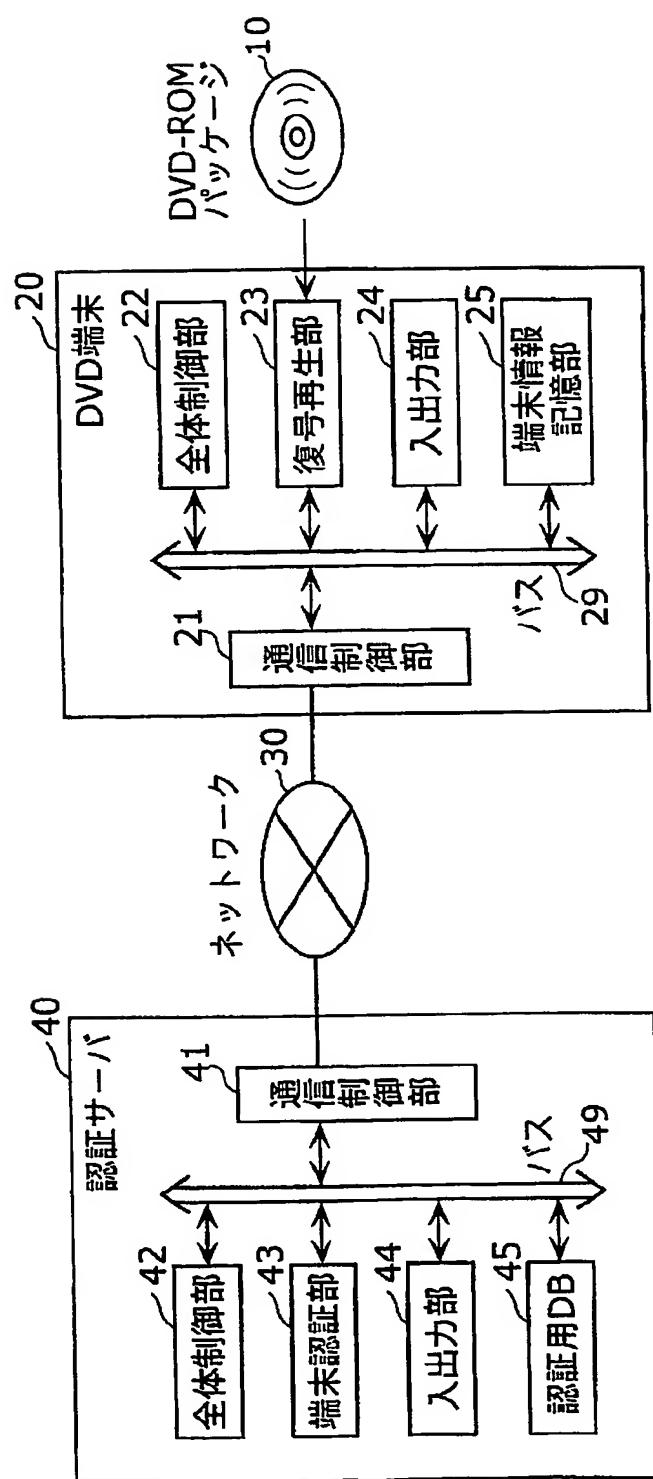
【0049】

5	不正端末検出システム
1 0	DVD-ROMパッケージ
2 0	DVD端末
2 1	通信制御部
2 2	全体制御部
2 3	復号再生部
2 4	入出力部
2 5	端末情報記憶部
3 0	ネットワーク
4 0	認証サーバ
4 1	通信制御部
4 2	全体制御部
4 3	端末認証部
4 4	入出力部
4 5	認証用DB
5 0	センタ
1 0 0	機器製造メーカー
1 5 0	ライセンサ
2 0 0	機器製造メーカー
3 0 0	機器製造メーカー

【書類名】 図面
【図 1】



【図 2】



【図 3】

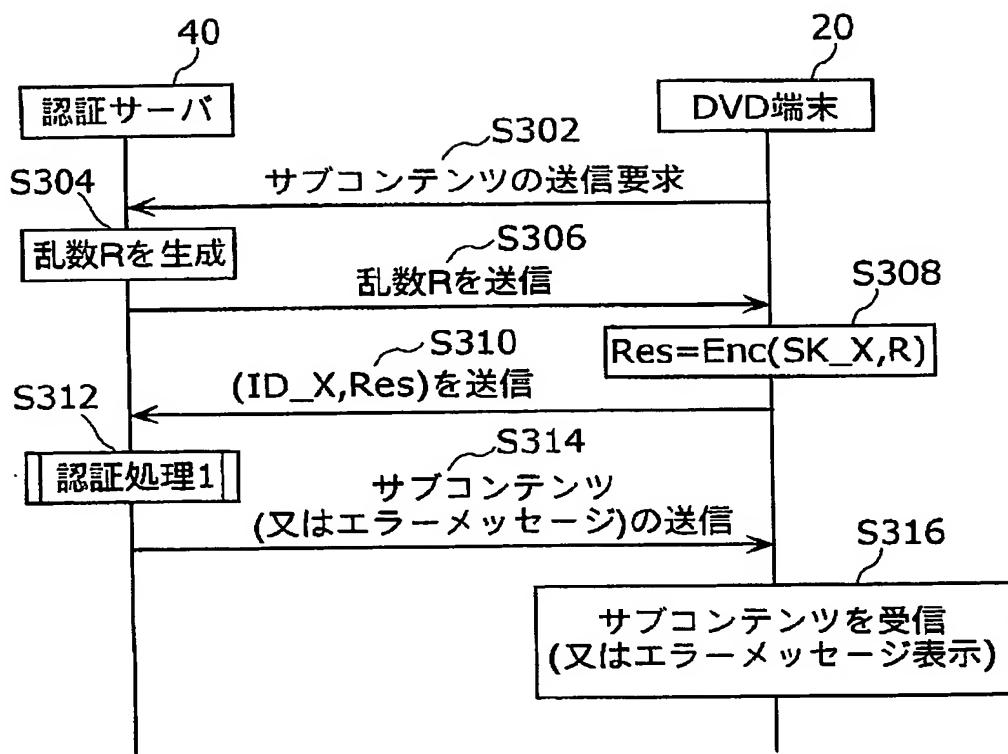
(a)

形式+連番	端末ID	端末鍵	サブコンテンツのダウンロード履歴
DVM-1234-NNNNN	ABC5566	DEF7890	○○○ディレクターズカット版
DVM-2345-NNNNN	UVW6677	XYZ8901	△△△メイキングフィルム
⋮	⋮	⋮	⋮

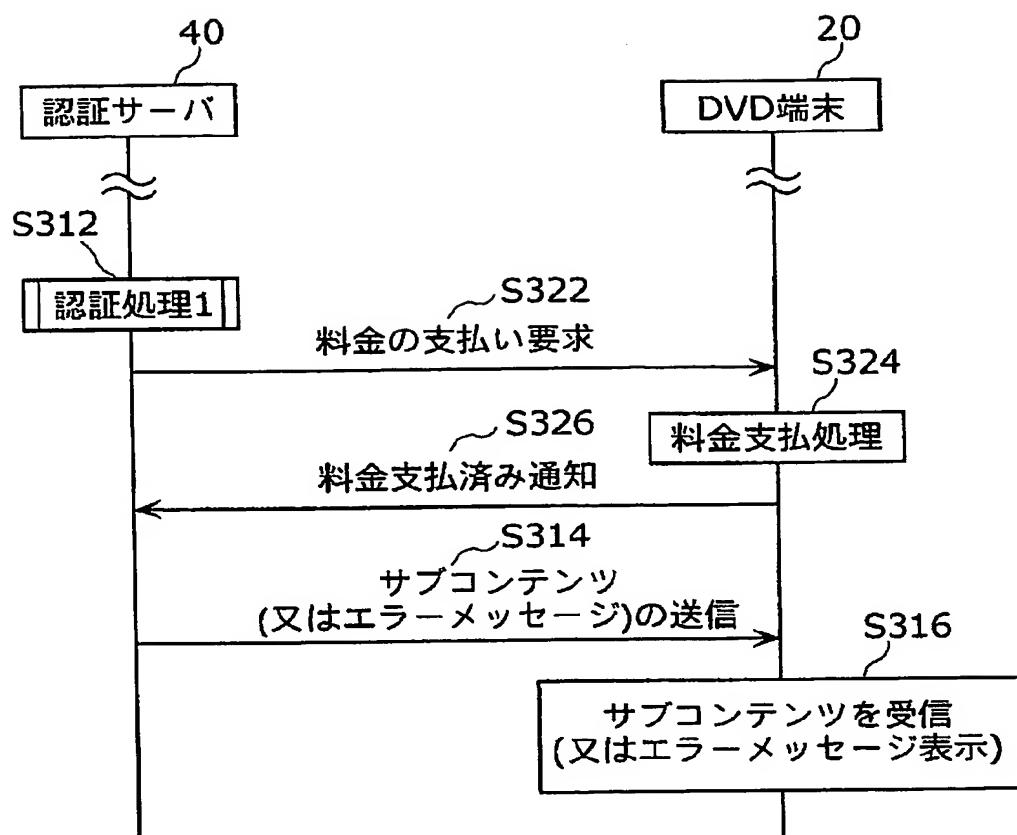
(b)

形式	端末鍵の総数	アクセス数
DVM-1234	10,000	18,500
DVM-5678	50,000	36,200
⋮	⋮	⋮

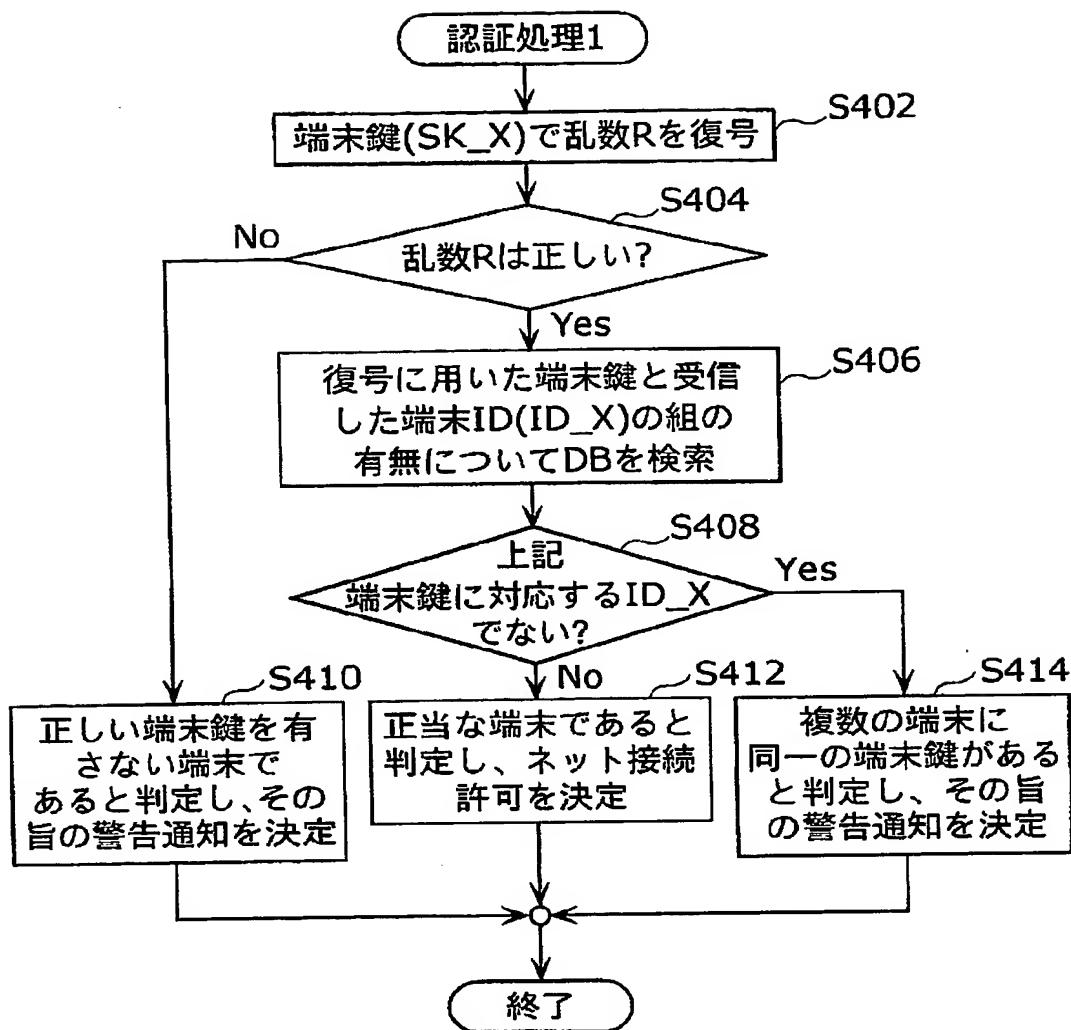
【図4】



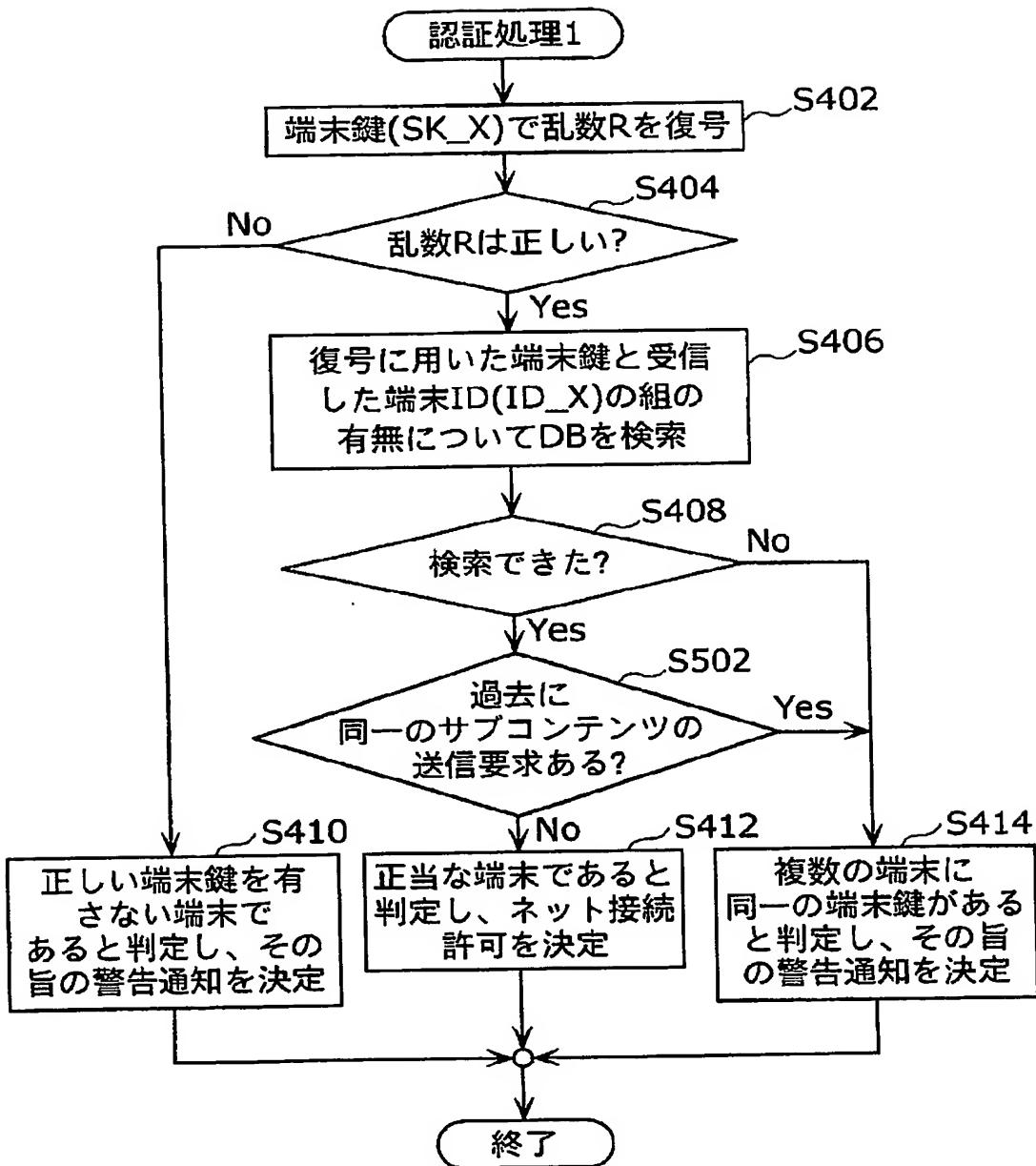
【図5】



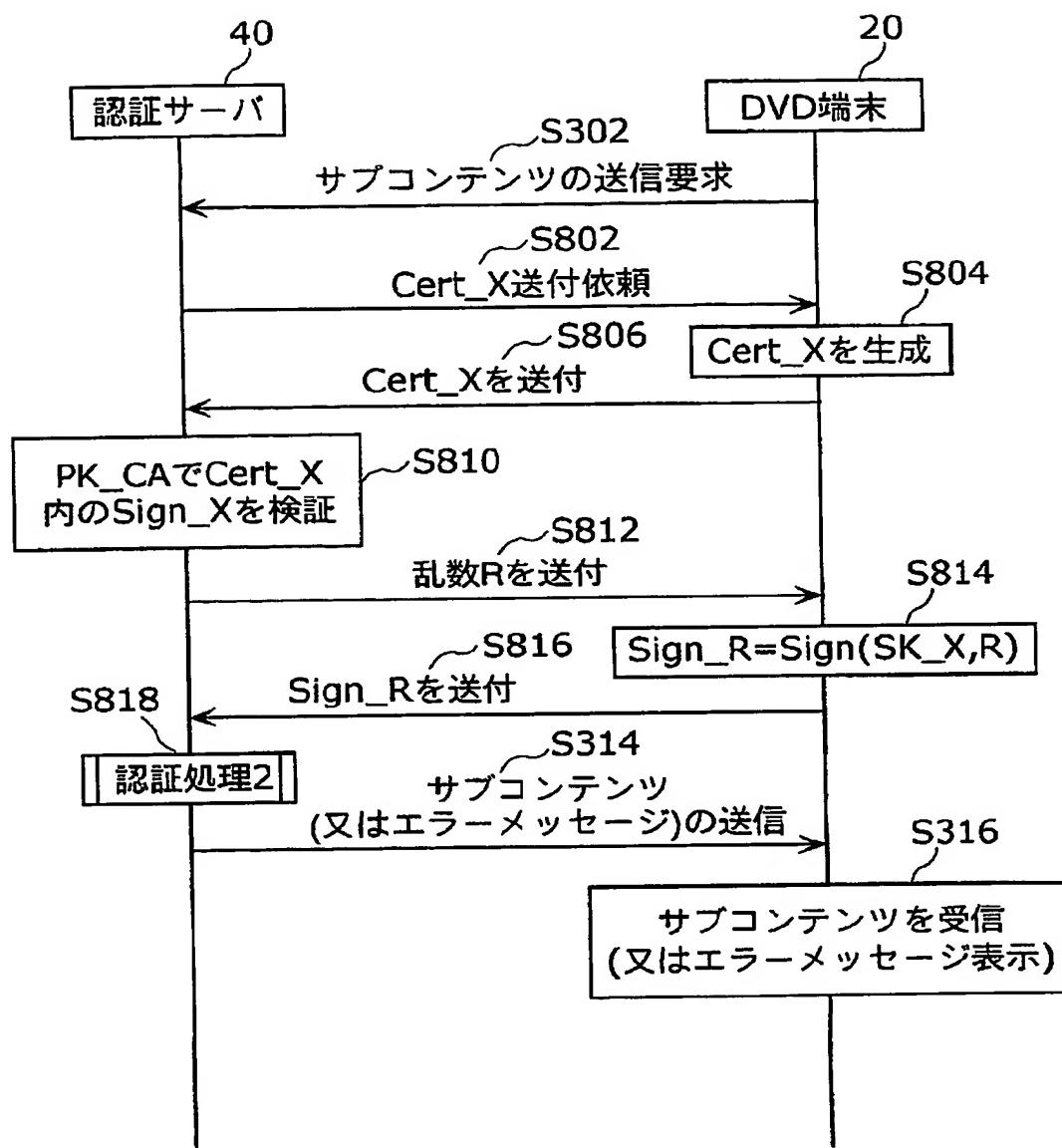
【図6】



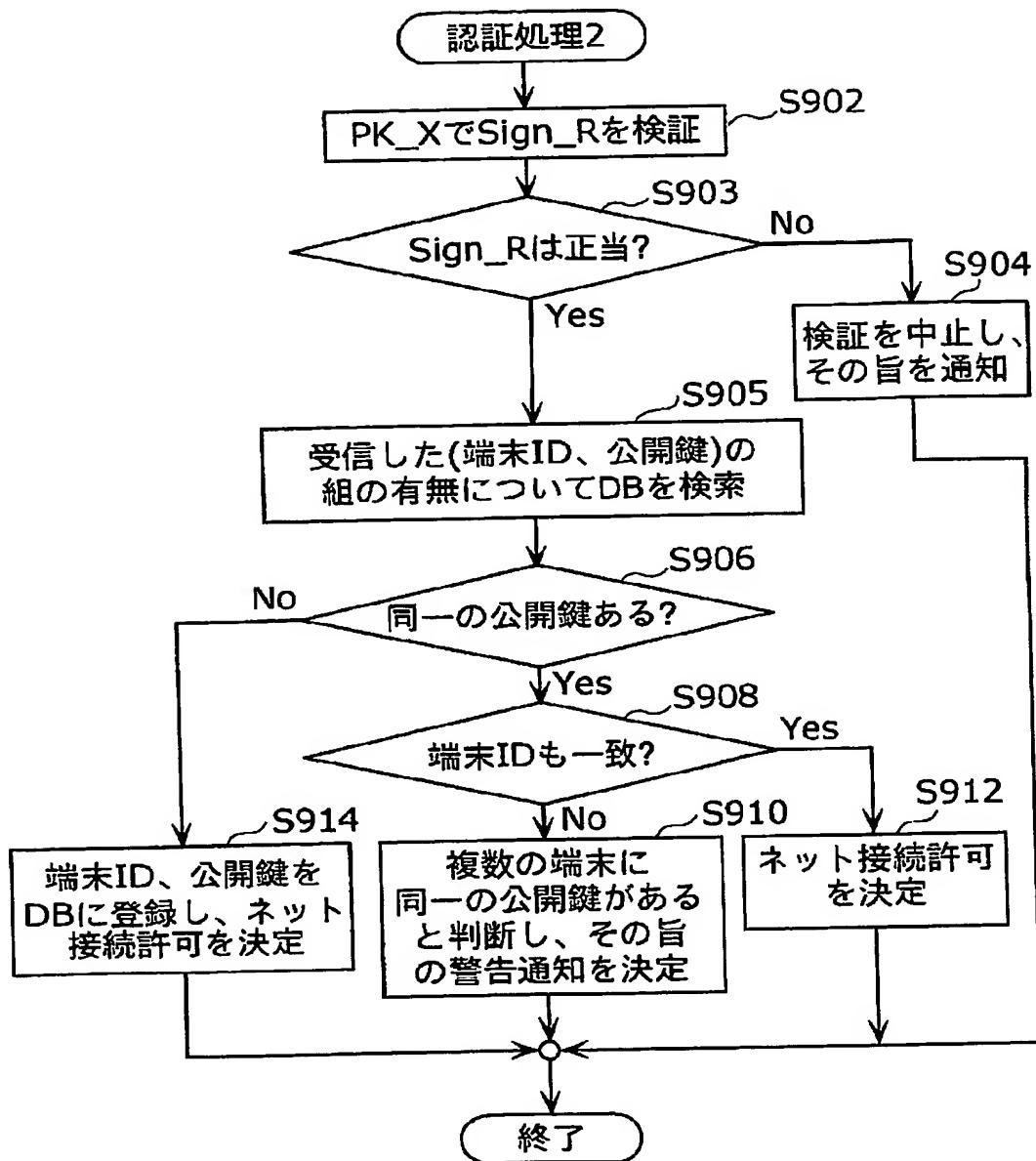
【図 7】



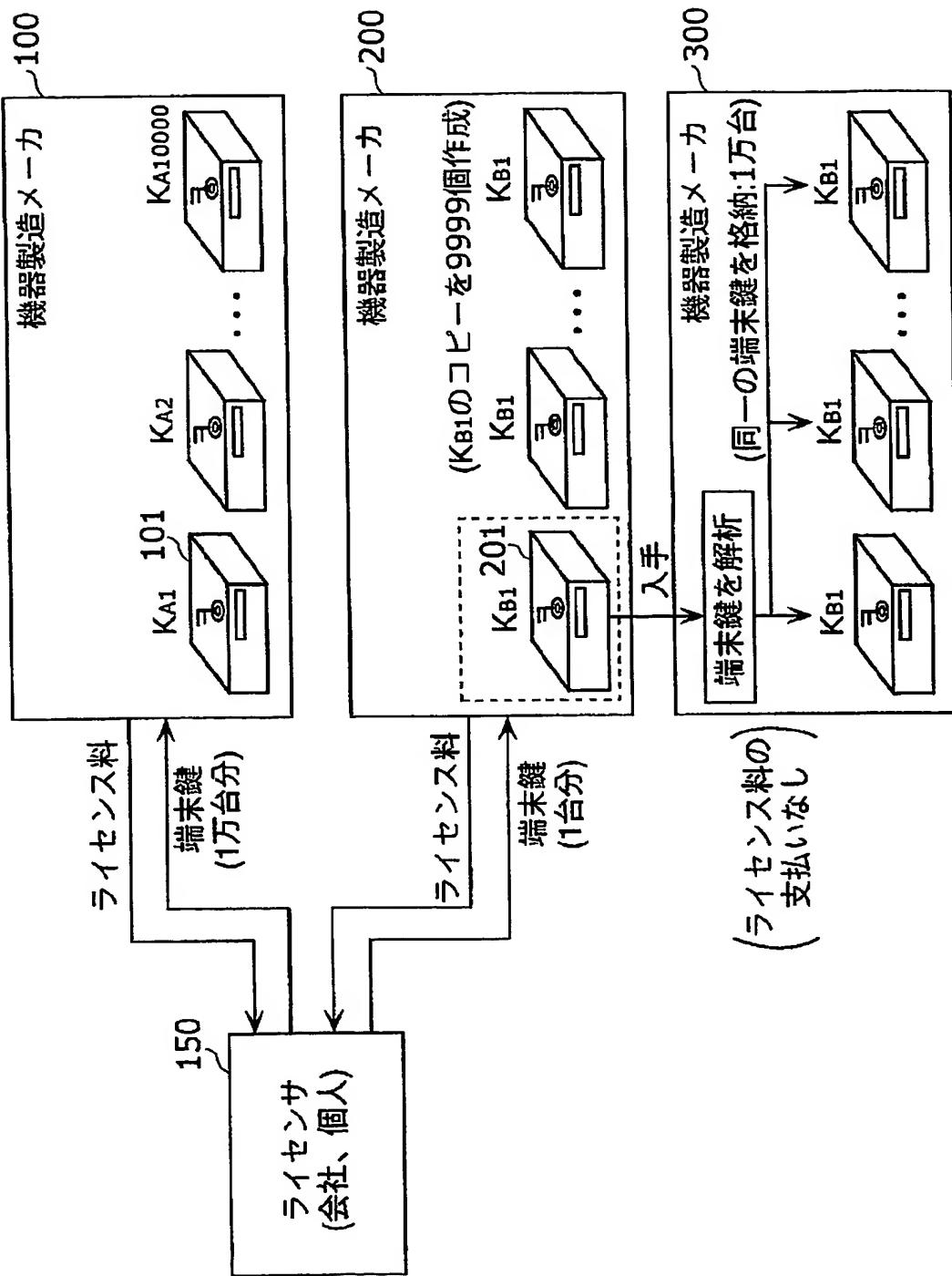
【図 8】



【図9】



【図10】



【書類名】要約書

【要約】

【課題】 複数の端末に同一の端末鍵が格納されていることや不正端末にどの正当な端末の端末鍵が格納されているかを検出し得る認証用サーバ装置、不正端末検出方法などを提供する。

【解決手段】 DVD端末20は、認証サーバ40にサブコンテンツの送信要求を行う（S302）。認証サーバ40は、乱数Rを生成し（S304）、DVD端末20に送信する（S306）。DVD端末20は、端末情報記憶部25に記憶している端末鍵と端末IDを読み出し、端末鍵（SK_X）で、受信した乱数Rを暗号化し（S308）、これと端末ID（ID_X）とを認証サーバ40に送信する（S310）。認証サーバ40は、DVD端末20から受信した暗号化された乱数R及び端末IDについて検証し、DVD端末20が正当な端末か否かを認証する（S312）。

【選択図】 図4

認定・付加情報

特許出願の番号	特願2004-009861
受付番号	50400073755
書類名	特許願
担当官	第七担当上席 0096
作成日	平成16年 1月19日

<認定情報・付加情報>

【提出日】 平成16年 1月16日

特願 2004-009861

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住所 大阪府門真市大字門真1006番地
氏名 松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019488

International filing date: 20 December 2004 (20.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-009861
Filing date: 16 January 2004 (16.01.2004)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse